UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,509	12/12/2003	Sudarshan Palliyil	JP920030270US1	5856

39903 7590 01/28/2009

IBM ENDICOTT (ANTHONY ENGLAND)
LAW OFFICE OF ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/735,509
Filing Date: December 12, 2003
Appellant(s): PALLIYIL ET AL.

Anthony V.S. England
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/23/2008 appealing from the Office action mailed 03/13/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7143113	**Radatti**	**11-2006**
20050022018	**Szor**	**1-2005**

Takeshi Okamoto, Yoshiteru Ishida; A Distributed Approach against Computer Viruses Inspired by the Immune System; IEICE Trans. Commun; Vol. E83 B, No. 5; May 2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24-29, 31-36 and 38-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti (US 7,143,113) in view of Szor (US 2005/0022018).

Regarding claim 24:

Radatti discloses a method comprising the steps of:

computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas are stored on respective data processing systems within a network [*column 3 lines 17-34, the baseline is formed from the master system, all of the subsequent systems are replicas of the master system; therefore hash values derived from a master system represent a plurality of replicas*];

a) storing the computed first hash values [*column 3 lines 44-48, the secure system data is retained in a storage area, either internally or externally*];

b) computing current hash values for the replicas of the resource [*column 5 lines 28-34, in the comparison cycle, files are taken one at a time and hashed (MD5)*];

c) comparing the current and first hash values in order to identify whether all the hash values match, wherein nonmatching first and current hash values for a respective one of the replicas indicates the respective one of the replica has changed since the computing of the first hash value [*column 5 lines 33-58, the recent hash is compared with the old hash*];

d) detecting that a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas [*column 7 lines 54-58, if an unauthorized user changes the contents, the files modified by the virus will differ*]; and

e) presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number being exceeded [*column 7 lines 24-28, reporting may be used; as is well known in the art it is inherent that the reporting will take place after detection*].

Radatti does not disclose wherein the predetermined number is at least one. Szor is similar to Radatti in that Szor provides a method for network intrusion detection. Szor discloses a local analysis center (LAC) that receives notification packets about malicious code [*paragraphs 102-104*]. The LAC then checks to see if an attack threshold has been exceeded which is incremented by one for each notification packet [*paragraphs 108-109*] then appropriate action is taken [*paragraph 113*]. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Radatti to include the functionality of the LAC of Szor in order to determine a minimum level of suspicious activity [*paragraph 108*].

Regarding claim 25:

Radatti and Szor disclose the method of claim 24, wherein steps a), b), c), and d) are performed at a first data processing system within the network [Radatti, *column 3 lines 26-34, the secure system state and secure system data file are generated on the master system; column 6 lines 11-16, the client comparison may take place internally or externally; Radatti also discloses (column 3 lines 8-16) putting an individual computer in "lock down" and scanning for a baseline (in this case a, b, c, and d are performed inside a single computer)*].

Regarding claim 26:

Radatti and Szor disclose the method of claim 24, wherein step b) is performed at each replica's respective data processing system, the method further comprising sending the computed hash values to a first data processing system [Radatti, *column 6 lines 11-16, the hash values can be sent to an external processing system*].

Regarding claim 27:

Radatti and Szor disclose the method of claim 24, wherein the vulnerability includes a vulnerability to a computer virus [Radatti, *column 6 lines 17-38, compared against hashes of viruses*].

Regarding claim 28:

Radatti and Szor disclose the method of claim 24, wherein the vulnerability includes a vulnerability to computer hacking [Radatti, *column 6 lines 17-38, compared against hashes of Trojans and back doors*].

Regarding claim 29:

Radatti and Szor disclose the method of claim 24 further comprising:

classifying as vulnerable the data processing systems storing the replicas, wherein the classifying is responsive to the predetermined number or changed replicas of the resource being exceeded [Radatti, *column 9 lines 26-44, dangerous hash values are stored in the dangerous hash value data file, the comparison cycle will then compare new hashes with the dangerous hash file*].

Regarding claims 31-36 and 38-43:

Claims 31-36 and 38-43 are the system and computer program product corresponding to the method claims 24-29 and are rejected under the same reasoning.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 30, 37, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti and Szor as applied to claims 24, 31, and 38 above, and further in view of A Distributed Approach against Computer Viruses Inspired by the Immune System hereafter Immune System.

Radatti and Szor disclose the method of claim 24, the steps further comprising:

selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability [Radatti, *column 7 lines 59-65, the infected files may be restored to a known good state*].

Radatti and Szor do not disclose sending a notification of the vulnerability to each data processing system storing one of the replicas and sending the selected instructions to each of the data processing systems storing one of the replicas. Immune System teaches sending a notification of infection to other computers on the LAN to inform them of possible computer viruses (Page 912 – Section 3.3). Each computer in the LAN is programmed to scan its own file upon receiving notification of infection from another computer (Page 912 – Section 3.3). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Radatti and Szor with the notification system of Immune System in order to notify the other computers in the

network (Section 3.3.). Radatti, Szor or Immune System do not disclose sending selected instructions to each of the data processing systems storing one of the replicas, however, Radatti and Immune system are pre-programmed to handle the situation in which a notification of virus infection has occurred on another computer, then the two will scan their own files to ensure they are virus free. Sending instructions to a computer is well known in the art (JAVA, distributed processing systems, remote access and various other client-server models) and it would have been obvious to one of ordinary skill in the art to allow instructions to be received via the network instead of being pre-programmed in order to facilitate a more flexible reaction system to viruses and network intrusions.

(10) Response to Argument

Examiner respectfully disagrees with appellant regarding the arguments that:

1) Radatti teaches away from what is claimed

2) That the rejection relies on modifying the teaching of Szor regarding the functionality of the LAC

3) The rejection does not state a rational underpinning for the modification of both the teaching of Radatti and Szor

Regarding the argument of 1:

Radatti in column 7 lines 47-58 is not teaching away from the claims. The replicas in this instance are the system in which the files reside. The predetermined number in the instance of Radatti is zero as in if there aren't any modifications to the system or the files on that system, then there is no vulnerability. Szor adds the

functionality of the LAC to collect these notifications from each system when the individual systems determine they have a vulnerability, and the LAC has a threshold limit (greater than one) that determines when a vulnerability exists in the group of systems.

Regarding the argument of 2:

The teachings of Szor are being applied to Radatti. The teachings of Szor in the specification are exemplary embodiments of the invention and the scope of the invention is not limited by the exemplary embodiments [*paragraph 149 of Szor*]. Appellants are arguing the exact components and teachings of the exemplary embodiments while the examiner relied upon the teachings of the LAC to receive notification packets about malicious code and check to see if an attack threshold has been exceeded which is incremented by one for each notification packet. The combination of the two teachings, Radatti and Szor, results in a method and apparatus that detects a change in the local replica, sends a notification to LAC, similar to the LAC of Szor, and the LAC determines when a threshold has been met and whether or not there is a security vulnerability.

Regarding the argument of 3:

The substitution of "determining a minimum suspicious level" for "detecting that a vulnerability exists" in order to present that the examiner is using circular logic is spurious. Examiner does not interpret “detecting that a vulnerability exists” as “determining a minimum suspicious level”. The examiner states in the rejection, "It would have been obvious to one of ordinary skill in the art at the time of invention to

modify the method of Radatti to include the functionality of the LAC of Szor in order to determine a minimum level of suspicious activity [*paragraph 108*]." The determining a minimum level of suspicious activity is the motivation of the obviousness statement.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

James Turchen

/James Turchen/

Conferees:

/Andrew L Nalven/

Primary Examiner, Art Unit 2434

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434